PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2000-099403**

(43)Date of publication of application : **07.04.2000**

(51)Int.Cl. **G06F 12/14**

(21)Application number : **10-265210** (71)Applicant : **FUJITSU LTD**

(22)Date of filing : **18.09.1998** (72)Inventor : **KOTANI MASATAKE**
HASEBE TAKAYUKI
HIRANO HIDEYUKI

(54) **METHOD AND DEVICE FOR MANAGING INFORMATION**

(57)Abstract:

PROBLEM TO BE SOLVED: To enable a user to restore granted information destructed due to some faults by backup information by enciphering prescribed information on a recording medium by information inherent in the medium or a key generated based on the inherent information and leading out the enciphered information to the outside of a prescribed area.

SOLUTION: A driving device 31 is provided with a writing/reading means 32 for writing/reading out optional information 7 in/from a 3rd hierarchy 4 to be a user using area and a prescribed information leading-out means 33 for enciphering prescribed information 6 stored in a 2nd hierarchy 3 to be a secret area by using an inherent medium number 5 stored in a 1st hierarchy 2 and leading out the enciphered information to the outside of the 2nd hierarchy 3. Since an enciphered composite key is constituted so as to be led out to the outside of the

prescribed area, the key can be stored as a user's backup data. Since the user can restore the composite key by using the backup data, the user can restore granted information even when it is destructed.

LEGAL STATUS

[Date of request for examination]	27.10.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3819160
[Date of registration]	23.06.2006
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] The information management approach which enciphers with the key generated based on the information on said medium proper, or it, and derives the predetermined information stored in the predetermined field on the record

medium which has the information on a medium proper outside said predetermined field.

[Claim 2] Said record medium is the information management approach [equipped with the 1st field which stores said predetermined information, and said 1st field and the 2nd different field] according to claim 1.

[Claim 3] It is the information management approach according to claim 2 which is the secret field [said 2nd field is a user use field which can read / a store and / the information on arbitration based on the command from the outside, and] which cannot control said 1st field based on the command from the outside.

[Claim 4] The predetermined information which the information on the arbitration stored in said 2nd field is enciphered electronic data, and is stored in said 1st field is the information management approach including the consent information based on the right of use using said electronic data according to claim 3.

[Claim 5] Said predetermined information is the information management approach according to claim 2 to 4 which is enciphered with the key generated based on the information on said medium proper, or it, and is stored in said predetermined field.

[Claim 6] Said predetermined information is the information management approach according to claim 5 enciphered with the key generated by the equipment which drives said record medium based on the information on a proper, or it.

[Claim 7] The information management approach according to claim 2 to 6 of storing said information on predetermined [which was enciphered] in said 2nd field.

[Claim 8] The information management approach according to claim 7 which decrypts the information on predetermined [which was enciphered] stored in said 2nd field with the key generated based on the information on said medium proper, or it, and updates the predetermined information stored in said 1st field.

[Claim 9] The information management approach according to claim 7 enciphered with the key generated by the equipment which drives the key

generated based on the information on said medium proper, or it, and said record medium in case said predetermined information is derived outside said 1st field based on the information on a proper, or it.

[Claim 10] The information management approach according to claim 9 which decrypts the information on predetermined [which was enciphered] stored in said 2nd field with the key generated based on the information on the key generated by the equipment which drives said record medium based on the information on a proper, or it, and said medium proper, or it, and updates the predetermined information stored in said 1st field.

[Claim 11] The information management approach given in whether it is the gap of claims 1-6 which stores said information on predetermined [which was enciphered] on the 2nd record medium from which said record medium differs.

[Claim 12] The information management approach according to claim 11 which decrypts the information on predetermined [which was enciphered] stored in said 2nd record medium with the key generated based on the information on said medium proper, or it, and updates the predetermined information stored in said predetermined field.

[Claim 13] The information management approach according to claim 11 enciphered with the key generated by the equipment which drives the key generated based on the information on said medium proper, or it, and said 2nd record medium in case said predetermined information is derived on said 2nd record medium based on the information on a proper, or it.

[Claim 14] The information management approach according to claim 13 which decrypts the information on predetermined [which was enciphered] stored in said 2nd record medium with the key generated based on the information on the key generated by the equipment which drives said 2nd record medium based on the information on a proper, or it, and said medium proper, or it, and updates the predetermined information stored in said predetermined field.

[Claim 15] The information on said medium proper is the information management approach given in claims 1-14 currently displayed on said record

medium in visible while being able to obtain electronically from said record medium at either.

[Claim 16] It is the information management approach according to claim 6, 9, or 10 currently displayed on it on said equipment in visible while the information on a proper can come to hand to the equipment which drives said record medium electronically from said equipment.

[Claim 17] It is the information management approach according to claim 13 or 14 currently displayed on it on said equipment in visible while the information on a proper can come to hand to the equipment which drives said 2nd record medium electronically from said equipment.

[Claim 18] It has the information on a medium proper and is based on a command from the outside. The user use field which can read [a store and] the information on arbitration, It has the secret field which cannot be controlled based on the command from the outside. The consent information based on the right of use to the information on the arbitration stored in said user use field is information management equipment which manages the information on the record medium stored in said secret field. The store and a read-out means to perform store and read-out for the information on arbitration to said user use field, Information management equipment equipped with a predetermined information derivation means to encipher the consent information stored in said secret field with the key generated based on the information on said medium proper, or it, and to derive outside said secret field.

[Claim 19] Information management equipment according to claim 18 which stores said enciphered consent information in said user use field with said store and read-out means.

[Claim 20] Information management equipment according to claim 19 further equipped with a renewal means of predetermined information to update the consent information which decrypts the enciphered consent information which is stored in said user use field using the information on said medium proper, and is stored in said secret field.

[Claim 21] It is information management equipment according to claim 18 or 19 as which said predetermined information derivation means enciphers said consent information by having the information on an equipment proper with the key generated by the key generated based on the information on said medium proper, or it, and said equipment based on the information on a proper, or it.
[Claim 22] The information-management equipment according to claim 21 further equipped with a renewal means of predetermined information update the consent information which decrypts the enciphered consent information which is stored in said user use field with the key generated based on the information on the key generated by said equipment based on the information on a proper, or it, and said medium proper, or it, and is stored in said secret field.
[Claim 23] Said predetermined information derivation means is information management equipment according to claim 18 which sends out to the 2nd record medium with which said record media differ said enciphered consent information.
[Claim 24] Information management equipment according to claim 23 further equipped with a renewal means of predetermined information to update the consent information which decrypts the enciphered consent information which is stored in said 2nd record medium using the information on said medium proper, and is stored in said secret field.
[Claim 25] It is information management equipment according to claim 23 which enciphers said predetermined information derivation means with the key generated by the equipment which drives the key generated based on the information on said medium proper, or it in said consent information, and said 2nd record medium based on the information on a proper, or it by equipping with the information on an equipment proper the equipment which drives said 2nd record medium.
[Claim 26] The information-management equipment according to claim 25 further equipped with a renewal means of predetermined information update the consent information which decrypts the enciphered consent information which is stored in said 2nd record medium with the key generated based on the information on the

key generated by the equipment which drives said 2nd record medium based on the information on a proper, or it, and said medium proper, or it, and is stored in said secret field.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention relates the information on arbitration to the information management approach at the time of performing record and read-out, and its equipment about the information management approach and information management equipment to the record medium which has the information on a medium proper.

[0002]

[Description of the Prior Art] By software and electronic publishing objects, such as a computer program, electronic data are stored on a magneto-optic disk (MO), a digital video disc (DVD), a floppy disk (FD), a mini disc (MD), and other record media, and it is sold. Generally such electronic data are easy to copy, and the illegal copy is performed frequently. For this reason, there is a possibility that it may infringe on the copyright by the side of a software vendor or a publisher, and profits may be checked remarkably.

[0003] In order to protect the electronic data stored on such a record medium, the consent information which used the information on a user proper and was enciphered is generated, and storing this in the predetermined field on a record medium, and distributing it is proposed. It is enciphered by the predetermined cryptographic key and electronic data, such as software and a publication, are stored on the record medium. Moreover, it is enciphered using the information on a user proper, and the decode key for decrypting this enciphered electronic data

is stored on the record medium as consent information.

[0004] In a user side, by decrypting this consent information using the information on a user proper, a decode key can be obtained, and the enciphered electronic data which are stored on the record medium can be decrypted and used using this decode key. Thus, in case the right of use of electronic data is granted to user each by constituting, the cryptographic key for enciphering electronic data can be carried out in common, and it becomes possible by enciphering a decode key using the information on a different user proper for every user to grant the right of use separately.

[0005] The information on the user proper used here is the device number given to the equipment which drives the computer or record medium which the user is using. Therefore, even if a user receives to normal, with different equipment, it becomes impossible to use it and there is un-arranging [that this record medium cannot be transferred, either]. The approach which enciphers the decode key for giving the information on this medium proper to a record medium, and decoding the enciphered electronic data using the information on this medium proper, and was stored in the record medium is proposed by JP,5-257816,A.

[0006] In this case, the cryptographic key at the time of enciphering electronic data can be carried out in common like the above-mentioned case, and it becomes possible by enciphering a decode key using the information on a different medium proper for every user to grant the right of use separately.

[0007]

[Problem(s) to be Solved by the Invention] The enciphered electronic data are stored in the field where a user is accessible in the above approaches. Moreover, the consent information for using this electronic data is stored in the secret field which a user cannot access. Even if it is the user of normal, consent information cannot be read and backup cannot be taken, but when the data stored in this secret field are destroyed by a certain failure, it becomes impossible therefore, to use electronic data. In such a case, the recurrence line of the right of use by the manager of electronic data, such as a software vendor, and a publisher, its

agency, is needed. Therefore, a complicated activity and excessive cost will be needed for the procedure of this recurrence line.

[0008] Even if this invention is the case where consent information required in order to use the electronic data stored on the record medium is destroyed by a certain failure, it aims at offering the information management approach with a user able to return this using backup information, and information management equipment.

[0009]

[Means for Solving the Problem] It enciphers with the key generated based on the information on a medium proper, or it, and the information management approach concerning this invention derives the predetermined information stored in the predetermined field on the record medium which has the information on a medium proper outside a predetermined field. Here, a record medium can be considered as a configuration equipped with the 1st field which stores predetermined information, and the 1st field and the 2nd different field.

[0010] Moreover, the 2nd field is a user use field which can read [a store and] the information on arbitration based on the command from the outside, and the 1st field can consist of secret fields which cannot be controlled based on the command from the outside. In this case, the information on the arbitration stored in the 2nd field is enciphered electronic data, and the predetermined information stored in the 1st field can be constituted so that the consent information based on the right of use using electronic data may be included.

[0011] Moreover, predetermined information can be considered as the configuration which is enciphered with the key generated based on the information on a medium proper, or it, and is stored in a predetermined field. Furthermore, predetermined information may be a configuration enciphered by the equipment which drives a record medium based on the information on a proper. Moreover, it can consider as the configuration which stores the enciphered predetermined information in the 2nd field.

[0012] In this case, the information on predetermined [which was enciphered]

stored in the 2nd field is decrypted with the key generated based on the information on a medium proper, or it, and it can constitute so that the predetermined information stored in the 1st field may be updated. Moreover, in case predetermined information is derived outside the 1st field, it can constitute so that it may encipher with the key generated by the equipment which drives the key and record medium which were generated based on the information on a medium proper, or it based on the information on a proper, or it.

[0013] In this case, the information on predetermined [which was enciphered] stored in the 2nd field is decrypted with the key generated based on the information on the key generated by the equipment which drives a record medium based on the information on a proper, or it, and a medium proper, or it, and it can constitute so that the predetermined information stored in the 1st field may be updated. Since it is enciphered by this medium using the information on a proper when deriving outside the predetermined field in which predetermined information is stored by considering as the above configurations, even if it copies to other record media, it is difficult to decrypt this. For example, if it enciphers by the cryptographic key and this electronic data is stored, and the decode key for decoding this is enciphered for the information on a proper to this record medium and it stores in the 1st field which cannot access a user in case electronic data, such as software and a publication, are stored in the 2nd field, it is not necessary to change the cryptographic key for enciphering into user each, and can encipher and store using a common cryptographic key. Since the enciphered decode key which is stored in the 1st field is constituted so that it may be further enciphered using the information on a medium proper and may derive outside the 1st field, it can be saved as backup of a user. Since it is enciphered by the information on a medium proper, this saved backup data is difficult to decrypt, even if it copies this to other record media, and it is difficult data to obtain the decode key for decoding electronic data.

[0014] Moreover, even if the information stored in the predetermined field is destroyed, it is possible to restore consent information by the user side based on

this backup data, and procedure of the recurrence line of the troublesome right of use is not needed. Moreover, it can constitute so that the enciphered predetermined information may be stored on the 2nd different record medium from a record medium.

[0015] In this case, the information on predetermined [which was enciphered] stored in the 2nd record medium is decrypted with the key generated based on the information on a medium proper, or it, and it can constitute so that the predetermined information stored in the predetermined field may be updated. Moreover, in case predetermined information is derived on the 2nd record medium, it can constitute so that it may encipher with the key generated by the equipment which drives the key and the 2nd record medium which were generated based on the information on a medium proper, or it based on the information on a proper, or it.

[0016] In this case, the information on predetermined [which was enciphered] stored in the 2nd record medium is decrypted with the key generated based on the information on the key generated by the equipment which drives the 2nd record medium based on the information on a proper, or it, and a medium proper, or it, and it can constitute so that the predetermined information stored in the predetermined field may be updated. Moreover, being displayed on a record medium in visible is desirable while the information on a medium proper can come to hand electronically from a record medium, and it is desirable to be displayed on it on equipment in visible, while the information on a proper can come to hand to the equipment which drives the information and the 2nd record medium of a proper to the equipment which drives a record medium electronically from equipment.

[0017] In this case, the backup data of consent information which was mentioned above are saved at the 2nd record medium, and when the data stored in the 1st field are destroyed, based on the information stored in this 2nd record medium, it becomes possible to restore this. The information management equipment concerning this invention has the information on a medium proper, and it is

based on a command from the outside. The user use field which can read [a store and] the information on arbitration, It has the secret field which cannot be controlled based on the command from the outside. The consent information based on the right of use to the information on the arbitration stored in the user use field is information management equipment which manages the information on the record medium stored in the secret field. It has a predetermined information derivation means to encipher the consent information stored in the store and a read-out means to perform store and read-out, and the secret field, in the information on arbitration to a user use field with the key generated based on the information on a medium proper, or it, and to derive outside a secret field.

[0018] Here, enciphered consent information can be considered as the configuration stored in a user use field with a store and a read-out means. Moreover, it can consider as the configuration further equipped with a renewal means of predetermined information to update the consent information which decrypts the enciphered consent information which is stored in the user use field using the information on a medium proper, and is stored in the secret field.

[0019] Furthermore, it has the information on an equipment proper, and a predetermined information derivation means can be constituted so that consent information may be enciphered with the key generated by the key generated based on the information on a medium proper, or it, and equipment based on the information on a proper, or it. In this case, it can consider as the configuration further equipped with a renewal means of predetermined information to update the consent information which decrypts the enciphered consent information which is stored in the user use field using the information on the key generated by equipment based on the information on a proper, or it, and a medium proper, and is stored in the secret field.

[0020] Moreover, a predetermined information derivation means can be constituted so that the enciphered consent information may be sent out to the 2nd different record medium from a record medium. In this case, it can consider as the configuration further equipped with a renewal means of predetermined

information to update the consent information which decrypts the enciphered consent information which is stored in the 2nd record medium using the information on a medium proper, and is stored in the secret field.

[0021] Moreover, the equipment which drives the 2nd record medium is equipped with the information on an equipment proper, and a predetermined information derivation means can be constituted so that it may encipher with the key generated by the equipment which drives the key and the 2nd record medium which were generated based on the information on a medium proper, or it in consent information based on the information on a proper, or it. In this case, it can consider as the configuration further equipped with a renewal means of predetermined information to update the consent information which decrypts the enciphered consent information which is stored in the 2nd record medium using the information on the key generated by the equipment which drives the 2nd record medium based on the information on a proper, or it, and a medium proper, and is stored in the secret field.

[0022]

[Embodiment of the Invention] The operation gestalt of this invention is explained with reference to a drawing.

[Record medium] The record media used for this invention are a magneto-optic disk (MO), a digital video disc (DVD), a floppy disk (FD), a mini disc (MD), and a record medium that can rewrite the data by other users, for example, explain the record section by drawing 1 about a magneto-optic disk.

[0023] Although the record medium 1 is possible for read-out by the user, it has the 1st hierarchy 2 who cannot rewrite, the 2nd hierarchy 3 in whom read-out and the writing by the command from the outside are impossible, and the 3rd hierarchy 4 with a user able to write information in arbitration. The medium specific number 2 determined as a meaning about the medium is stored in the 1st hierarchy 2. The 3rd hierarchy 4 is a field where a user is able to store the information 7 on arbitration, and is a user contents field which stores a computer program for a user to use, an electronic publishing object, and the other data of

arbitration. The 2nd hierarchy 3 is a field for storing the predetermined information 6 based on the information on the arbitration stored in the 3rd hierarchy 4, for example, the consent information based on rights of use stored in the 3rd hierarchy 4, such as a computer program and an electronic publishing object, etc. is stored.

[Configuration by the side of consent] In case electronic data are stored and distributed to a record medium, when setting up the right of use for using this electronic data for every user, this electronic data is enciphered and it stores in a record medium. For example, as shown in drawing 2 , when it stores electronic data in a record medium 11, the contents 17 enciphered by the consent information 16 based on [based on the medium specific number 15 to the 1st hierarchy 12] the right of use to the 2nd hierarchy 13 and the 3rd hierarchy 14 are stored. Here, the consent information 16 is data based on a user's right of use, for example, can be used as the decode key for decrypting the enciphered contents 17.

[0024] By computer 21 by the side of consent, it has the individual key generation means 22, the consent information encryption means 23, the contents encryption means 24, the cryptographic key table 25, the decode key table 26, etc. The contents encryption means 24 enciphers the data 27 which serve as contents by the cryptographic key of the cryptographic key table 25, and stores them in the 3rd hierarchy 14 of a record medium 11 as contents. The decode key corresponding to the cryptographic key of the cryptographic key table 25 is stored in the decode key table 26. The individual key generation means 22 generates a medium individual key based on the medium specific number 15 read from the 1st hierarchy 12 of a record medium 11. The consent information encryption means 23 enciphers the decode key of the decode key table 26 with a medium individual key, and stores it in the 2nd hierarchy 13 of a record medium 11 as consent information 16.

[Configuration by the side of a user] The driving gear by the side of the user for driving the record medium 1 of drawing 1 is shown in drawing 4 as the

conceptual block diagram.

[0025] The driving gear 31 is equipped with a predetermined information derivation means 33 enciphers as the store and a read-out means 32 to perform writing of the information 7 on arbitration, and read-out to the 3rd hierarchy 4 who is a user use field, using the medium specific number 5 in which the predetermined information 6 stored in the 2nd hierarchy 3 who is a secret field is stored by the 1st hierarchy 2, and derive to fields other than 2nd hierarchy 3. As a location where the predetermined information derivation means 33 enciphers and derives predetermined information, such as consent information, the 3rd hierarchy 4 or other record media can be considered, for example. When it stores the enciphered consent information in the 3rd hierarchy 4 of a record medium 1, it can be made to store as information 7 on arbitration with a store and the read-out means 32.

[0026] A simplified block diagram is shown in drawing 4 as an example of a still more concrete configuration. The driving gear 41 by the side of a user is equipped with the individual key generation means 42, the consent information decryption means 43, the decode key storing section 44, the contents decryption means 45, the decode data storage section 46, the consent information encryption means 47, etc. The individual key generation means 42 generates the same thing as the individual key which generates a medium individual key based on the medium specific number 15 stored in the 1st hierarchy 12 of a record medium 11, and is generated by the individual key generation means 22 by the side of consent. The consent information decryption means 43 reads the consent information 16 stored in the 2nd hierarchy 13 of a record medium 11, and decrypts it with the individual key generated by the individual key generation means 42. The consent information decrypted by the consent information decryption means 43 is temporarily stored in the decode key storing section 44. The contents decryption means 45 reads the contents 17 stored in the 3rd hierarchy 14 of a record medium 11, decrypts them using the decode key stored in the decode key storing section 44, and is stored in the decode data storage

section 46.

[0027] The consent information encryption means 47 reads the 2nd hierarchy's 13 consent information 16, and enciphers it using the medium specific number 12 stored in the 1st hierarchy 12. In this case, it is also possible to use the medium specific number 12 as it is, it is also possible to encipher using the individual key generated with the individual key generation means 42, and it is also possible to generate a cryptographic key based on the medium specific number 12, and to encipher further, using this. Then, the enciphered consent information is stored in the 3rd hierarchy 14 of a record medium 11.

[Contents storing processing] The actuation at the time of storing electronic data in a consent side at a record medium 11 is shown in drawing 5 as a flow chart.

[0028] At step S1, the computer program stored in a record medium 11, an electronic publishing object, and other electronic data are created. At step S2, the cryptographic key for enciphering electronic data is created. At step S3, the electronic data and the cryptographic key which encipher are made to correspond, and it stores in the cryptographic key table 25. At this time, the decode key for decoding the data enciphered by the cryptographic key by coincidence is created, electronic data and a decode key are made to correspond, and it stores in the decode key table 26. It is also possible to make a cryptographic key and a decode key common and to use the cryptographic key table 25 and the decode key table 26 as one key managed table.

[0029] In step S4, the cryptographic key corresponding to the electronic data which encipher is taken out from the cryptographic key table 25. At step S5, electronic data are enciphered by the cryptographic key. For example, in using a DES code, it enciphers by repeating substitution and bit transposition to the electronic data which encipher. At step S6, it stores in the 3rd hierarchy 14 of a record medium 11 by making the enciphered electronic data into contents 17. At step S7, it distinguishes whether storing of the enciphered electronic data was completed. When all storing of the enciphered electronic data is completed, it shifts to step S8.

[0030] At step S8, the medium specific number 15 is read from the 1st hierarchy 12 of a record medium 11, and an individual key is generated. In step S9, the decode key corresponding to the electronic data stored in the record medium 11 as contents 17 is read from the decode key table 26, and it enciphers with the individual key generated at step S8. After enciphering all the decode keys corresponding to the electronic data stored as contents 17, in step S10, this enciphered decode key is made into the consent information 16, and it stores in the 2nd hierarchy 13 of a record medium 11.

[Decryption processing of electronic data Since it is enciphered by the cryptographic key which the consent side created, in order to use this by the user side, it is necessary to decrypt the contents 17 stored in the 3rd hierarchy 14 of a record medium 11 with a suitable decode key.] The actuation at this time is explained using the flow chart of drawing 6 . If a driving gear 41 is equipped with a record medium 11 and the load instruction of data is made, in step S21, the medium specific number 15 will be read from the 1st hierarchy 12 of a record medium 11. At step S22, an individual key is generated from the medium specific number 15. Here, the same algorithm as step S8 by the side of consent generates an individual key. At step S23, it decrypts using the individual key which read the consent information 16 stored in the 2nd hierarchy 13 of a record medium 11, and generated this at step S22. The consent information decrypted here is a decode key for decrypting contents 17, it is made to correspond with the electronic data in which this decode key is stored to the 3rd field 14, is used as a decode key table, and stores this in the decode key storing section 44 temporarily.

[0031] At step S24, the contents 17 stored in the 3rd hierarchy 14 of a record medium 11 are read. At step S25, the read contents 17 are decrypted using the decode key stored in the decode key storing section 44. The decrypted contents are performed at step S26.

[Backup process of consent information] In the driving gear 41 by the side of a user, the consent information 16 stored in the 2nd hierarchy 13 of a record

medium 11 is saved as backup data. This processing is explained using drawing 7 .

[0032] At step S31, the consent information 16 stored in the 2nd hierarchy 13 of a record medium 11 is read. At step S32, the read consent information 16 is enciphered by the medium specific number 15. At this time, it is also possible to encipher consent information 16 using the individual key generated by step 22, and it is also possible to constitute so that it may encipher using the key which enciphered the medium specific number 15 with other algorithms. At step S33, the enciphered consent information 16 is stored in the 3rd hierarchy 14 of a record medium 11.

[0033] If the backup data in the 3rd hierarchy 14 are read and it returns the 2nd hierarchy 13 when the 2nd hierarchy's 13 consent information 16 is destroyed since backup of the consent information 16 is saved in the 3rd hierarchy 14 in such a configuration, it will become possible to use contents 17, without waiting for the recurrence line of the consent information 16. Moreover, since it is enciphered by the medium specific number 15, even if the similar copy of the contents stored in the 3rd hierarchy 14 of a record medium 11 is carried out, the consent information saved to the 3rd hierarchy 14 is difficult for restoring the consent information 16 on original, and can prevent unjust use of contents 17. Operation gestalt] besides [

(A) When the consent information 16 stored in the 2nd hierarchy 13 of a record medium 11 is destroyed, explain the case where the driving gear which drives a record medium 11 is equipped with the function which restores the consent information 16 using the backup data of consent information saved to the 3rd hierarchy 14. Drawing 8 is the control-block Fig. of such a driving gear 51, and the individual key generation means 42, the consent information decryption means 43, the decode key storing section 44, the contents decryption means 45, the decode data storage section 46, and the consent information encryption means 47 are the same as that of the operation gestalt shown in drawing 4 , and omit explanation.

[0034] The renewal means 52 of consent information reads the enciphered consent information which is saved to the 3rd hierarchy 14 of a record medium 11, and decrypts it by the medium specific number 15 in which this is stored by the 1st hierarchy 12. Here, when the consent information saved to the 3rd hierarchy 14 is enciphered with the individual key generated by the individual key generation means 42, as for the key used for a decryption, this individual key will be used. Then, the decrypted consent information is stored in the 2nd hierarchy 13 of a record medium 11 as consent information 16.

[0035] Actuation of this operation gestalt is shown in drawing 9 as a flow chart. At step S41, the enciphered consent information which is stored in the 3rd hierarchy 14 of a record medium 11 is read. At step S42, the read consent information which was enciphered is decrypted by the medium specific number 15. It is also possible to decrypt consent information using the individual key generated by step 22 at this time, and when enciphered using the key which enciphered the medium specific number 15 with other algorithms, it decrypts using this key. At step S43, the decrypted consent information is stored in the 2nd hierarchy 13 of a record medium 11 as consent information 16.

[0036] The consent information 16 stored in the 2nd hierarchy 13 of a record medium 11 by this can be restored using the enciphered consent information which is saved as backup data to the 3rd hierarchy 14, when a certain failure breaks. Processing of the consent information 16 not being outputted outside and using this information unjustly since this restoration processing is processed within a driving gear 51

(B) The operation gestalt in the case of enciphering further by the equipment specific number of a proper is shown in the driving gear for driving a record medium 11 at drawing 10 - drawing 12 .

[0037] As shown in drawing 10 , in a driving gear 61, the individual key generation means 42, the consent information decryption means 43, the decode key storing section 44, the contents decryption means 45, the decode data storage section 46, and the consent information encryption means 47 are the

same as that of the operation gestalt shown in drawing 4 , and omit explanation. Moreover, the driving gear 61 is equipped with the equipment specific number storing section 62 which stores an equipment specific number. Furthermore, it has the 2nd consent information encryption means 63. This 2nd consent information encryption means 63 enciphers further the consent information enciphered by the medium specific number 15 with the consent information encryption means 47 by the equipment specific number. The consent information enciphered by this 2nd consent information encryption means 63 is stored in the 3rd hierarchy 14 of a record medium 11.

[0038] Moreover, the driving gear 61 is equipped with the renewal means 64 of consent information. This renewal means 64 of consent information reads the enciphered consent information which is saved to the 3rd hierarchy 14 of a record medium 11. A 1st consent information restoration means 65 to decrypt by the equipment specific number in which this is stored by the equipment specific number storing section 62, It has a 2nd consent information restoration means 66 to decrypt by the medium specific number 15 in which the consent information which the 1st consent information restoration means 65 decrypted is stored by the 1st hierarchy 12 of a record medium 11. The restored consent information is stored in the 2nd hierarchy 13 as consent information 16 on a record medium 11.

[0039] It is performed by the procedure shown in drawing 11 in case backup of the consent information 16 stored in the record medium 11 is saved. First, at step S51, the consent information 16 stored in the 2nd hierarchy 13 of a record medium 11 is read. At step S52, it enciphers by the medium specific number 15 in which the read consent information 16 is stored by the 1st hierarchy 12. At step S53, the consent information enciphered by the medium specific number 15 is enciphered by the equipment specific number in which it was stored by the equipment specific number storing section 62. Then, the enciphered consent information is stored in the 3rd hierarchy 14 in step S54.

[0040] When the consent information 16 stored in the record medium 11 is destroyed, the procedure shown in drawing 12 restores consent information. At

step S61, the enciphered consent information which is stored in the 3rd hierarchy 14 of a record medium 11 is read. At step S62, the read consent information which was enciphered is decrypted by the equipment specific number. At step S63, the consent information decrypted by the equipment specific number is decrypted by the medium specific number 15. At step S64, the decrypted consent information is stored in the 2nd hierarchy 13 of a record medium 11 as consent information 16.

[0041] Thus, since it is enciphered by the medium specific number 15 and the backup data of the consent information 16 are further enciphered by the equipment specific number of a driving gear 61 when constituted, even if it performs the illegal copy of data, it cannot use, but protection of copyrights can be carried out. Moreover, even if the consent information 16 on a record medium 11 is destroyed, restoring using this driving gear 61 is possible, and if it is the user of normal, use of contents will be attained, without waiting for a recurrence line.

[0042] Although the equipment specific number was made into the device number of a proper at the driving gear 61 for driving a record medium 11, it is also possible to use the device number of a proper for the computer currently used by the user side. Moreover, when it is also possible to encipher and store by the medium specific number 15 after enciphering by the equipment specific number, in case the backup data of the consent information 16 are saved and it restores this, after decrypting by the medium specific number 15, it will decrypt by the equipment specific number.

(C) It is also possible to save the backup data of the consent information 16 at other record media. Such an operation gestalt is explained based on drawing 13 - drawing 15 .

[0043] It connects with the driving gear 81 for driving the 2nd record medium 83, and an exchange of the data between media is possible for the driving gear 71 for driving a record medium 11. A floppy disk drive (FDD), the hard disk drive (HDD), the mini disc (MD), the magneto-optic disk (MO), the digital disk drive

(DVD), etc. were adopted, the driving gear 81 is equipped with the equipment specific number storing section 82 for storing an equipment specific number, and it is possible to output this equipment specific number as electronic data.

[0044] In the driving gear 71 which drives a record medium 11, the individual key generation means 42, the consent information decryption means 43, the decode key storing section 44, the contents decryption means 45, the decode data storage section 46, and the consent information encryption means 47 are the same as that of the operation gestalt shown in drawing 4 , and omit explanation. The driving gear 71 is further equipped with the 2nd consent information encryption means 72 and the renewal means 73 of consent information. The 2nd consent information encryption means 72 enciphers further the consent information enciphered by the consent information encryption means 47 by the equipment specific number of a driving gear 81. Then, the enciphered consent information is stored in the 2nd record medium 83.

[0045] The renewal means 73 of consent information reads the enciphered consent information which is saved at the 2nd record medium 83. A 1st consent information restoration means 74 to decrypt by the equipment specific number in which this is stored by the equipment specific number storing section 82, It has a 2nd consent information restoration means 75 to decrypt by the medium specific number 15 in which the consent information which the 1st consent information restoration means 74 decrypted is stored by the 1st hierarchy 12 of a record medium 11. The restored consent information is stored in the 2nd hierarchy 13 as consent information 16 on a record medium 11.

[0046] It is performed by the procedure shown in drawing 14 in case backup of the consent information 16 stored in the record medium 11 is saved. First, at step S71, the consent information 16 stored in the 2nd hierarchy 13 of a record medium 11 is read. At step S72, it enciphers by the medium specific number 15 in which the read consent information 16 is stored by the 1st hierarchy 12. At step S73, the consent information enciphered by the medium specific number 15 is enciphered by the equipment specific number of the driving gear 81 for driving

the 2nd record medium 83. Then, the enciphered consent information is stored in the 3rd hierarchy 14 in step S74.

[0047] When the consent information 16 stored in the record medium 11 is destroyed, restoration processing of the consent information 16 is performed by the procedure shown in drawing 15 . At step S81, the enciphered consent information which is stored in the 2nd record medium 83 is read. At step S82, the read consent information which was enciphered is decrypted by the equipment specific number of the driving gear 81 which drives the 2nd record medium 83. At step S83, the consent information decrypted by the equipment specific number is decrypted by the medium specific number 15. At step S84, the decrypted consent information is stored in the 2nd hierarchy 13 of a record medium 11 as consent information 16.

[0048] Thus, when constituted, the backup data of the consent information 16 can be separated from a record medium 11, and can be managed, and high security can be maintained. Moreover, it is possible about two or more record media to manage the consent information by the user side, and even if consent information is destroyed in a certain form, corresponding by the user side is possible. Here, in case the consent information 16 is enciphered, after enciphering by the equipment specific number, you may constitute so that it may encipher by the medium specific number. In this case, in case this is restored, after decrypting by the medium specific number, it will decrypt by the equipment specific number.

(D) The above approaches can be applied, when broadcasting the data enciphered in cable television, the Internet, etc. and making this record on a record medium by the user side. For example, the medium specific number of the record medium which recorded encryption data from the user side is made to transmit to a broadcasting station, and the decode key enciphered by the medium specific number is transmitted to a user. With the equipment by the side of a user, this decode key is stored as consent information of the 2nd hierarchy of a record medium. Furthermore, this consent information is enciphered by the

medium specific number, and it stores in the 3rd hierarchy.

[0049] What is necessary is to decrypt consent information by the medium specific number, to generate a decode key and just to decrypt the enciphered data, in using the contents on a record medium. Also in this case, even if it copies contents to other record media as it is, consent information is enciphered by the medium specific number and it is difficult to decrypt. Moreover, it is possible to restore consent information using backup data, and even if it is the case where consent information is destroyed, restoring by the user side is possible.

[0050]

[Effect of the Invention] According to this invention, even if it is enciphering and drawing the predetermined information stored in the predetermined field of a record medium using the information on a medium proper and copies to other record media, it is difficult to decrypt this. For example, if it enciphers by the cryptographic key and this electronic data is stored, and the decode key for decoding this is enciphered for the information on a proper to this record medium and it stores in the field which cannot access a user in case electronic data, such as software and a publication, are stored, it is not necessary to change the cryptographic key for enciphering into user each, and can encipher and store using a common cryptographic key. Since the enciphered decode key is constituted so that it may be further enciphered using the information on a medium proper and may derive outside a predetermined field, it can be saved as backup of a user. Since it is enciphered by the information on a medium proper, this saved backup data is difficult to decrypt, even if it copies this to other record media, and it is difficult data to obtain the decode key for decoding electronic data. Moreover, a user becomes possible [omitting the procedure of a recurrence line], even if data are the case where a certain failure is destroyed, since a decode key can be restored using this backup data.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The conceptual diagram showing the record section of the record medium used for this invention.

[Drawing 2] The simplified block diagram by the side of consent.

[Drawing 3] The conceptual block diagram of this invention.

[Drawing 4] The simplified block diagram of 1 operation gestalt.

[Drawing 5] The control flow chart of contents storing processing.

[Drawing 6] The control flow chart of decryption processing.

[Drawing 7] The control flow chart of a backup process.

[Drawing 8] The simplified block diagram of other operation gestalten.

[Drawing 9] The flow chart of a consent information update process.

[Drawing 10] The simplified block diagram of other operation gestalten.

[Drawing 11] The control flow chart.

[Drawing 12] The control flow chart.

[Drawing 13] The simplified block diagram of other operation gestalten.

[Drawing 14] The control flow chart.

[Drawing 15] The control flow chart.

[Description of Notations]

1 Record Medium

2 1st Hierarchy

3 2nd Hierarchy

4 3rd Hierarchy

5 Medium Specific Number

6 Predetermined Information

7 Information on Arbitration

11 Record Medium

12 1st Hierarchy

13 2nd Hierarchy

14 3rd Hierarchy

15 Medium Specific Number

16 Consent Information

17 Contents

21 Consent Side Computer

22 Individual Key Generation Means

23 Consent Information Encryption Means

24 Contents Encryption Means

25 Cryptographic Key Table

26 Decode Key Table

31 Driving Gear

32 Store and Read-out Means

33 Predetermined Information Derivation Means

41 Driving Means

42 Individual Key Generation Means

43 Consent Information Decryption Means

44 Decode Key Storing Section

45 Contents Decryption Means

46 Data Storage Section

47 Consent Information Encryption Means

52 Renewal Means of Consent Information

83 2nd Record Medium